PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-282430
(43)Date of publication of application : 07.10.1994

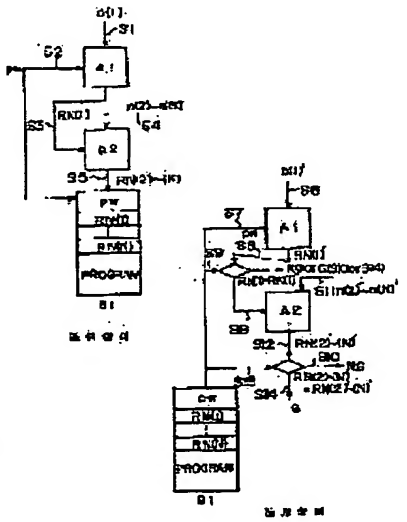
(51)Int.Cl. G06F 9/06
G06F 3/06
G06F 12/14

(21)Application number : 05-070322
(22)Date of filing : 29.03.1993

(71)Applicant : NEC CORP
(72)Inventor : SONEDAKA NORIYOSHI

(54) SOFTWARE COPY PROTECTION SYSTEM

(57)Abstract:
PURPOSE: To prevent a program from being executed, copied, or duplicated by an unregistered machine or to prevent illegal access from the same (internal) or an external network and the program from being executed, copied, or duplicated.
CONSTITUTION: Ciphered data S3 generated by ciphering a server machine characteristic number S1 that a program user side has in advance by optional ciphering algorithm A1 with a password S2 is held on an optionally specified storage medium B1 and ciphered data S5 ciphered by optional ciphering algorithm A2 with ciphered data S3 and a client machine characteristic number S4 is held on the storage medium B1; when the program is installed in a providing side server machine on the user side, the program is executed only on condition that ciphered data S8 outputted by reading the server machine characteristic number S6 out and ciphering it by the ciphering algorithm A1 with the password S7 on the storage medium B1 matches that on the storage medium B1.



LEGAL STATUS

[Date of request for examination]	30.03.1993
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2046058
[Date of registration]	25.04.1996
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's	

BEST AVAILABLE COPY

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－282430

(43)公開日　平成６年(1994)10月７日

(51)Int.Cl.*		識別記号	庁内整理番号	Ｆ１	技術表示箇所
Ｇ０６Ｆ	9/06	４５０　Ｈ	9367－5B		
	3/06	３０１　Ｍ	7165－5B		
	12/14	３２０　Ｂ	9293－5B		

審査請求　有　請求項の数３　ＯＬ　（全５頁）

(21)出願番号　特願平5－70322

(22)出願日　平成５年(1993)３月29日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　曽根高　則義
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　弁理士　後藤　洋介　（外２名）

(54)【発明の名称】　ソフトウェアコピープロテクションシステム

1

【特許請求の範囲】

【請求項1】 ソフトウエアプログラムの提供者側において、予めソフトウェア使用者側が保有するサーバーマシン固有番号を提供者側が秘密に保持しているパスワードで任意の暗号化アルゴリズム1で暗号化した暗号化データ1を任意に指定した記憶媒体に提供するプログラムと一緒に保持し、前記暗号化データ1とクライアントマシン固有番号で任意の暗号化アルゴリズム2で暗号化した暗号化データ2を前記記憶媒体に保持して使用者側に提供し、ソフトウェアプログラムの使用者側において、提供された前記プログラムを提供者側と同じ認識のサーバーマシンにインストールすると、自動的にインストールされたマシンのサーバーマシン固有番号を読みだして前記プログラム上の記憶媒体に保持してあったパスワードとで前記暗号化アルゴリズム1に従って暗号化して出力された暗号化データ3が前記記憶媒体に保持してある暗号化データ1と同じである場合にのみサーバーマシン上でプログラムを実行可能とすることを特徴とするソフトウェアコピープロテクションシステム。

【請求項2】 請求項1に記載のソフトウェアコピープロテクションシステムにおいて、上記プログラムがサーバーマシンにインストールされ、かつ、数台のクライアントマシンが上記サーバーマシンと同一又は外部からこのネットワークに何らかの方法で接続された場合において、 クライアントマシン側ではプログラムをインストールしてあるサーバーマシンにアクセスした場合、そのクライアントマシン固有番号と前記暗号化データ3で任意の暗号化アルゴリズム2で暗号化した暗号化データ4が前記記憶媒体に保持していた暗号化データ2と同じである場合にのみサーバーマシンにアクセス可能であり、クライアントマシン上でプログラムを実行可能とするソフトウェアコピープロテクションシステム。

【請求項3】 請求項1または請求項2に記載のソフトウェアコピープロテクションシステムにおいて、登録できる前記クライアントマシン固有番号は無限であることを特徴とするソフトウェアコピープロテクションシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、暗号化技術を用いて、ソフトウェアプログラムの不正アクセス及び複写（コピー）保護に関する。

【0002】

【従来の技術】従来から使用されているコピープロテクションシステムの1つは、ソフトウェアが最初にディスケット上に置かれている時にその位置がランダムに決定される付加情報をソフトウェア中に挿入するものである。これはオリジナルのコピー条件下でのみしか再生することができない。不法なコピーが試みられると、付加情報は消去され、それが存在しないことは、ソフトウェア中のプロセスによって検出される。

2

【0003】コピープロテクションシステムのもう1つは、ディスケット形式で配布される大量販売ソフトウェアの全部又は一部を暗号化するために暗号化を使用することである。これに関して、保護すべきソフトウェアの全部を暗号化及び解読することはコストがかかり過ぎるので、プログラム全体の暗号化は通常、メイン・フレム・システムに限定されている。

【0004】また、最近では2つのIDと暗号化の組み合わせでコピーを防止するシステムが、米国特許0820015号及び日本国特許昭64－44542号の公報に見いだされる。この発明は、図2および図3に示すように、パーソナルコンピュータ10とこれにより制御される磁気ディスク装置12とを具備し、パーソナルコンピュータ10が単独にCPU14内に所有するCPU識別子（CPUID）36と各自に配送されるシステムの磁気ディスク装置12上に供給元識別子（SID）28を置く。パーソナルコンピュータ10は、さらにディスクオペレーションシステムDOSおよびこれにより制御され前記磁気ディスク装置12を制御するディスク駆動装置18とを有している。実施する際に置いて、プログラム20は、 インストールモジュール21、初期化モジュール22、アプリケーションプログラム24、コピープロテクトモジュール26、供給元識別子（SID）28、チェック数記憶領域（CHKSTOR）30、及び暗号化モジュール（ENCRYPT）32を含んでいる。

【0005】前記暗号化モジュール32は、図3に示すように、有効性検査ステップ37と、暗号化ステップ39と、インストールステップ40と、比較機能46とを有している。パーソナルコンピュータ10は、暗号化モジュール32と磁気ディスク装置12との間の読取り機能38および書き込み機能42を有している。CPUID36及びSID28は、暗号化モジュール32の暗号化アルゴリズムに従ってチェック数（CHK）を作成するのに使われる。この手段によって作成されたチェック数（CHK）は、初期時においては任意のチェック数記憶領域（CHKSTOR）30内の位置44に一旦格納され、実行時にインストールするCPUID36とSID28から新たにチェック数（CHK）を作成し、暗号化モジュール32中の比較機能46に与えられる。次に初期時に格納されたチェック数CHK44と実行時に得た比較機能46を同一か否かを判定する。その結果が一致していなければ、比較機能46の出力は不一致を示す。

【0006】

【発明が解決しようとする課題】前記米国特許0820015号及び日本国特許昭64－44542号に係る発明は、マシン単体で使用する場合は有効と認められるが、初期時に目的とするソフトウェアをインストールされる

PAGE 91/130 * RCVD AT 4/20/2006 5:51:50 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/0 * DNIS:2738300 * CSID:718-544-8588 * DURATION (mm-ss):77-06

までではマシンが特定されない欠点があり、又、多数のマシンが内部及び外部のネットワークに接続された場合はソフトウェアへのアクセスが容易に実現されるといった問題が存在している。

【０００７】本発明の課題は、登録していないマシンでのプログラムの実行及び複写及び転写（コピー）を防止し、又は同一（内部）及び外部のネットワークからの不正アクセス、プログラムの実行及び複写及び転写（コピー）を防止することができるソフトウェアコピープロテクションシステムを提供することにある。

【０００８】

【課題を解決するための手段】本発明によれば、ソフトウエアプログラムの提供者側において、予めソフトウェア使用者側が保有するサーバーマシン固有番号を提供者側が秘密に保持しているパスワードで任意の暗号化アルゴリズム１で暗号化した暗号化データ１を任意に指定した記憶媒体に提供するプログラムと一緒に保持し、前記暗号化データ１とクライアントマシン固有番号で任意の暗号化アルゴリズム２で暗号化した暗号化データ２を前記記憶媒体に保持して使用者側に提供し、ソフトウェアプログラムの使用者側において、提供された前記プログラムを提供者側と同じ認識のサーバーマシンにインストールすると、自動的にインストールされたマシンのサーバーマシン固有番号を読みだして前記プログラム上の記憶媒体に保持してあったパスワードとで前記暗号化アルゴリズム１に従って暗号化して出力された暗号化データ３が前記記憶媒体に保持してある暗号化データ１と同じである場合にのみサーバーマシン上でプログラムを実行可能とすることを特徴とするソフトウェアコピープロテクションシステムが得られる。

【０００９】

【実施例】次に、本発明のソフトウェアコピープロテクションシステムを図１を参照して説明する。

【００１０】ソフトウェアプログラムの提供者側において、予めプログラムの使用者に使用者が保持しているサーバーマシンとクライアントマシンの固有番号を確認する。この固有番号はマシンの中のＣＰＵかＲＯＭに通常は保持されており、マシンの製造番号かＯＳＩで指示されいる物理レベル層又はそれ以上のレベル層で固有の番号である。

【００１１】プログラムの提供者側において、予めプログラム使用者側が保有するサーバーマシン固有番号ｎ（１）をＳ１として提供者側が秘密に保持しているパスワードｐｗであるＳ２で任意暗号化アルゴリズム１であるＡ１で暗号化した暗号化データであるＳ３をＲＮ（１）として任意に指定した記憶媒体Ｂ１に提供するプログラムと一緒に保持し、更に暗号化データＳ３とクライアントマシン固有番号ｎ（２）～（Ｎ）をＳ４として任意の暗号化アルゴリズム２であるＡ２で暗号化した暗号化データＳ５をＲＮ（２）～（Ｎ）として記憶媒体Ｂ１にＲＮ（１）の保管位置とは別の場所に保持して使用者側に提供する。

【００１２】ソフトウェアプログラムの使用者側において、提供されたプログラムを提供者側に提出したサーバーマシンにインストールすると、自動的にインストールされたサーバーマシン固有番号ｎ（１）′であるＳ６を読みだして記憶媒体Ｂ１に保持してあったパスワードｐｗであるＳ７（＝Ｓ２）で暗号化アルゴリズム１であるＡ１で暗号し、出力された暗号化データＲＮ（１）′であるＳ８と記憶媒体Ｂ１に保持してあるＲＮ（１）と同じならば一致情報ＧであるＳ１４を出力し、サーバーマシン上でプログラムを実行することが可能になる。一致しなければ不一致情報ＮＧをＳ１０として出力し、プログラムの実行を阻止する。

【００１３】上記プログラムがサーバーマシンにインストールされ、かつ、数台のクライアントマシンが上記サーバーマシンと同一（内部）又は外部からこのネットワークに何らかの方法で接続された場合において、クライアントマシン側ではソフトウェアをインストールしてあるサーバーマシンにアクセスした場合、そのクライアントマシン固有番号ｎ（２）′～（Ｎ）′であるＳ１１と暗号化データＳ８で任意の暗号化アルゴリズム２であるＡ２で暗号化したデータＳ１２と記憶媒体Ｂ１に保持して有る暗号化データＲＮ（２）～（Ｎ）であるＳ１３（＝Ｓ５）を比較し、同じならば一致情報ＧをＳ１４をして出力し、クライアントマシン上でプログラムを実行することが可能になる。一致していなければ不一致情報ＮＧをＳ１０として出力し、プログラムの実行を阻止する。

【００１４】

【発明の効果】本発明は、登録していないマシンでのプログラムの実行及び複写及び転写（コピー）を防止し、又は同一（内部）及び外部のネットワークからの不正アクセス、プログラムの実行及び複写及び転写（コピー）を防止することができる。

【図面の簡単な説明】

【図１】本発明の実施例を示すブロック図である。

【図２】従来のシステムの構成要素を説明するためのブロック図である。

【図３】従来のシステムのパーソナルコンピュータとディスク駆動装置との関係を示すブロック図である。

【符号の説明】

Ｓ１　サーバーマシン固有番号ｎ（１）

Ｓ２，Ｓ７　パスワードｐｗ（Ｓ２＝Ｓ７）

Ｓ３，Ｓ９　暗号化データＲＮ（１）（Ｓ３＝Ｓ９）

Ｓ４，Ｓ１１　クライアントマシン固有番号ｎ（２）～（Ｎ）

Ｓ５，Ｓ１３　暗号化データＲＮ（２）～（Ｎ）（Ｓ５＝Ｓ１３）

Ｓ６　サーバーマシン固有番号ｎ（１）′

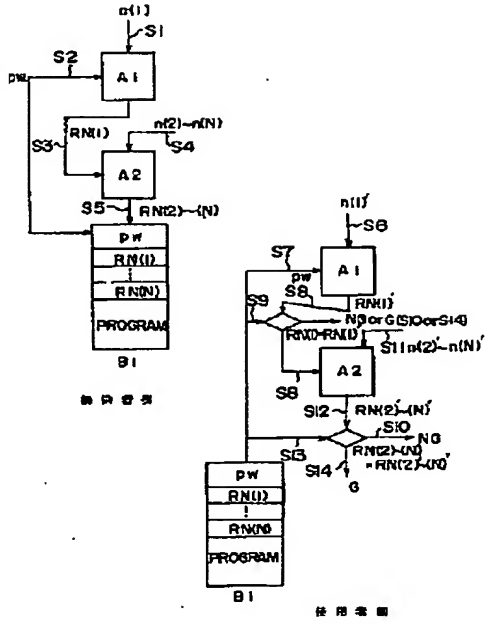
5

S8、S12　暗号化データRN（1）′、RN（2）′～（N）′
S10　不一致情報NG
S11　クライアントマシン固有番号n（2）′～（N）′
S14　一致情報G
A1，A2　暗号化アルゴリズム
B1　メモリ（暗号化データ記憶領域）
10　パーソナルコンピュータ
12　磁気ディスク装置
14　CPU
16　DOS
18　ディスク駆動装置
20　プログラム

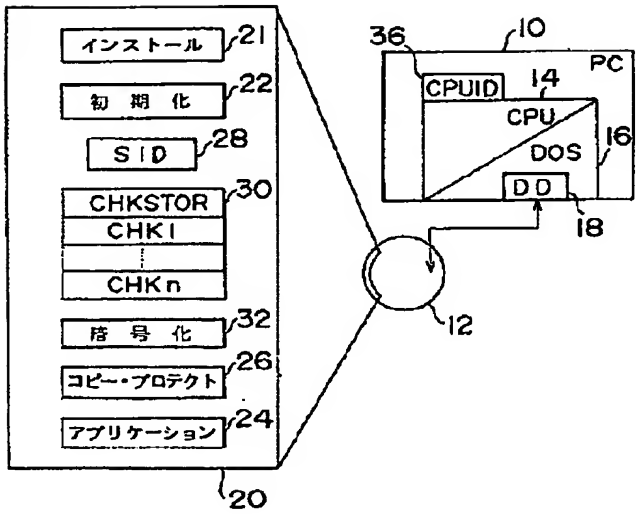
6

21　インストールモジュール
22　初期化モジュール
24　アプリケーションプログラム
26　コピープロテクトモジュール
28　SID（供給元識別子）
30　CHKSTOR（チェック数記憶領域）
32　暗号化モジュール
36　CPUID（CPU識別子）
38　読取機能
39　暗号化ステップ
42　書込機能
44　CHK位置格納機能
46　比較機能

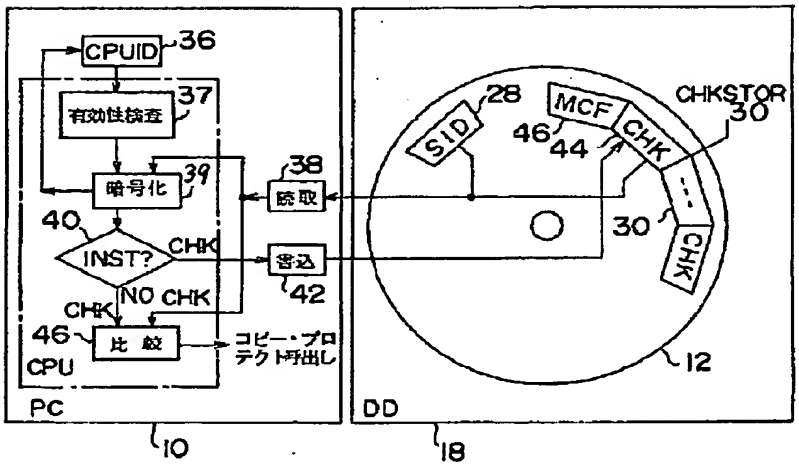
【図1】



【図2】



【図3】



PAGE 94/130 * RCVD AT 4/20/2006 5:51:50 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/0 * DNIS:2738300 * CSID:718-544-8588 * DURATION (mm-ss):77-06